

# 杭州电子科技大学

## 网络安全理论与技术实验

### 实 验 报 告

学 院	网络空间安全学院
专 业	网络工程
班 级	18272412
学 号	18041618
学生姓名	廖越强
教师姓名	高梦州
完成日期	11.2
成 绩	

## 实验一 OSPF 路由项攻击和防御实验

### 一、实验目的

1. 验证路由器 OSPF 配置过程
2. 验证 OSPF 建立动态路由项过程
3. 验证 OSPF 路由项欺骗攻击过程
4. 验证 OSPF 源端鉴别功能的配置过程
5. 验证 OSPF 防路由项欺骗攻击功能的实现过程

### 二、实验原理

路由项欺骗攻击过程如图 6.1 所示,入侵路由器伪造了和网络 192.1.4.0/24 直接连接的链路状态信息,导致路由器 R1 通过 OSPF 生成的动态路由项发生错误,如图 6.1 中 R1 错误路由表所示。解决路由项欺骗攻击问题的关键有三点:一是对建立邻接关系的路由器的身份进行鉴别,只和授权路由器建立邻接关系;二是对相互交换的链路状态信息进行完整性检测,只接收和处理完整性检测通过的链路状态信息;三是通过链路状态信息中携带的序号确定该链路状态信息不是黑客截获后重放的链路状态信息。实现上述功能的基础是在相邻路由器中配置相同的共享密钥,相互交换的链路状态信息和 Hello 报文携带由共享密钥加密的序号和由共享密钥生成的 MAC(消息鉴别码),通过消息鉴别码实现路由消息的源端鉴别和完整性检测,全部过程如图 6.2 所示。

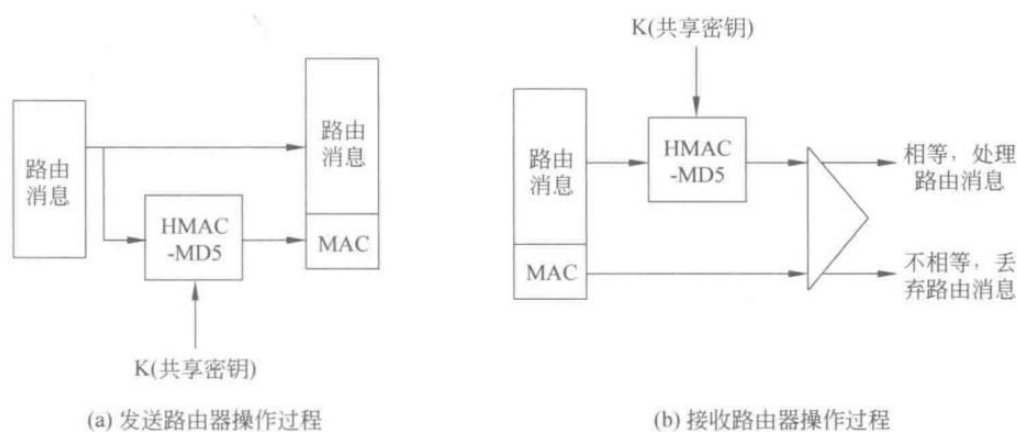
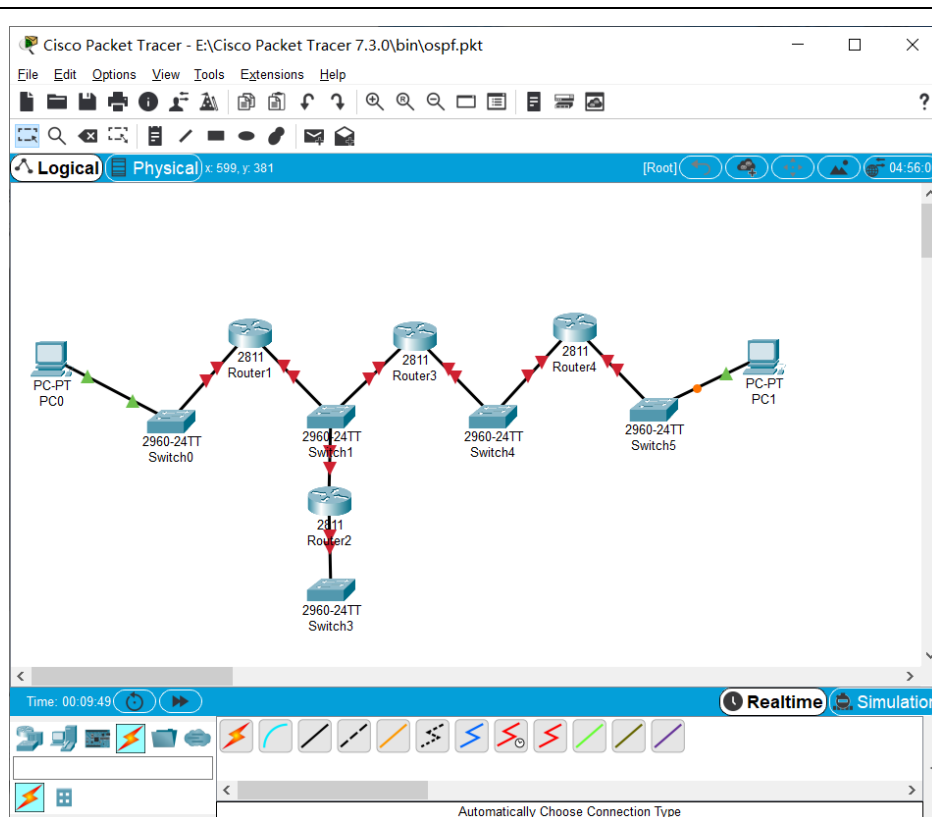


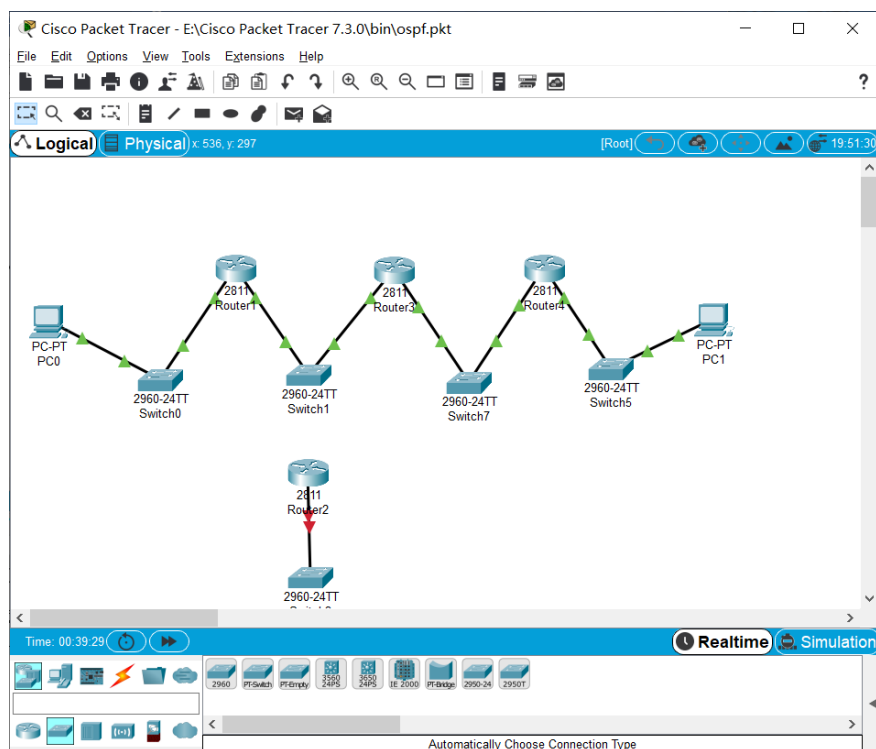
图 6.2 路由消息源端鉴别和完整性检测过程

### 三、实验环境/实验拓扑图

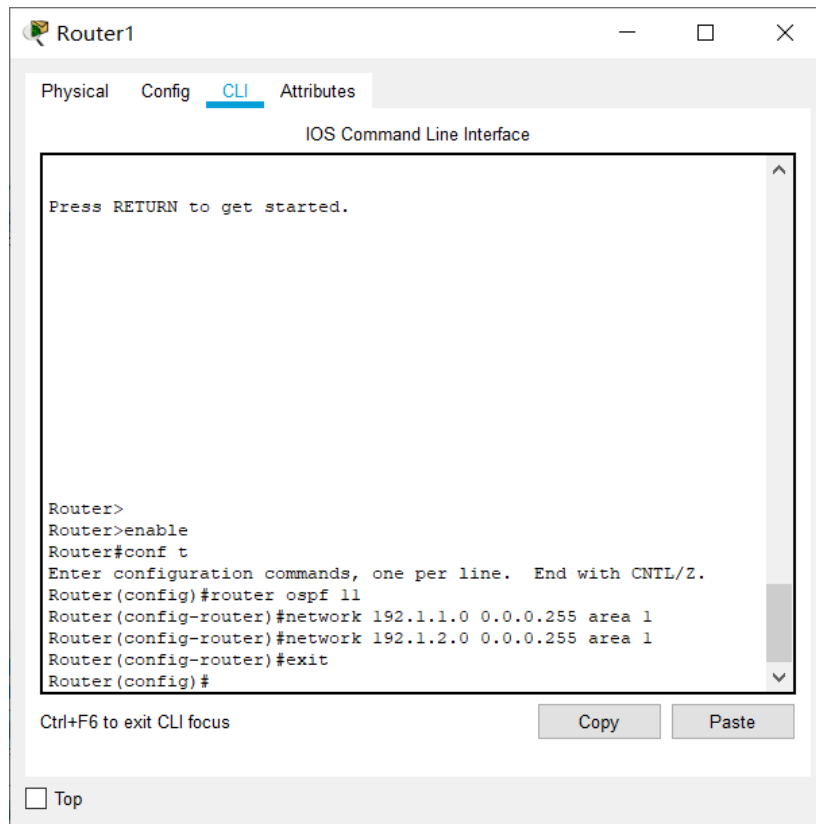


#### 四、 主要操作步骤及实验结果记录

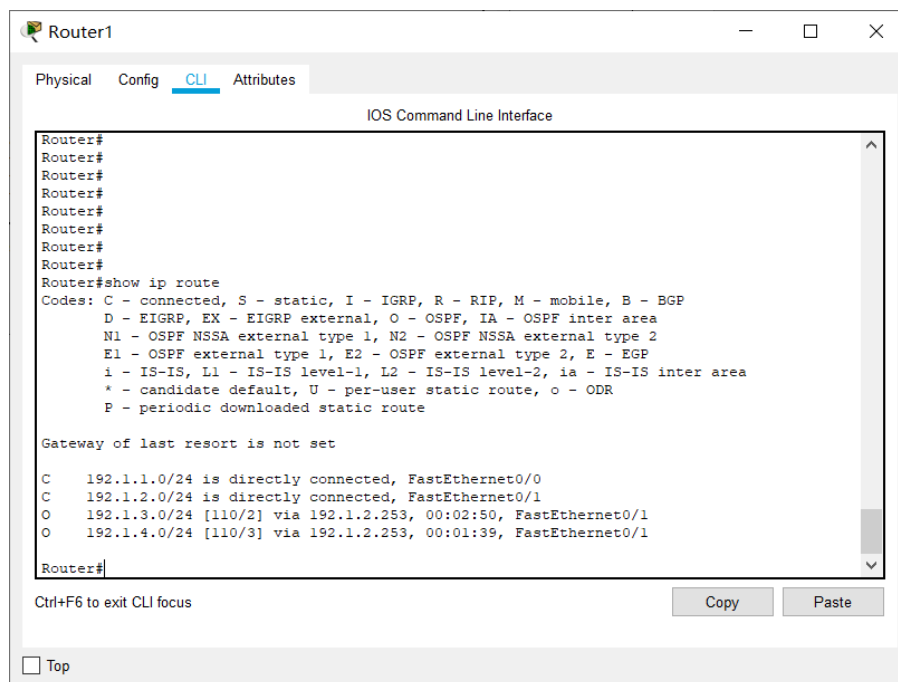
##### 1. 完成拓扑图连接



2. 完成网络信息配置（IP、掩码等），将除了入侵部分外的三个路由器都配置 ospf 功能，router1 配置如下，其余类似



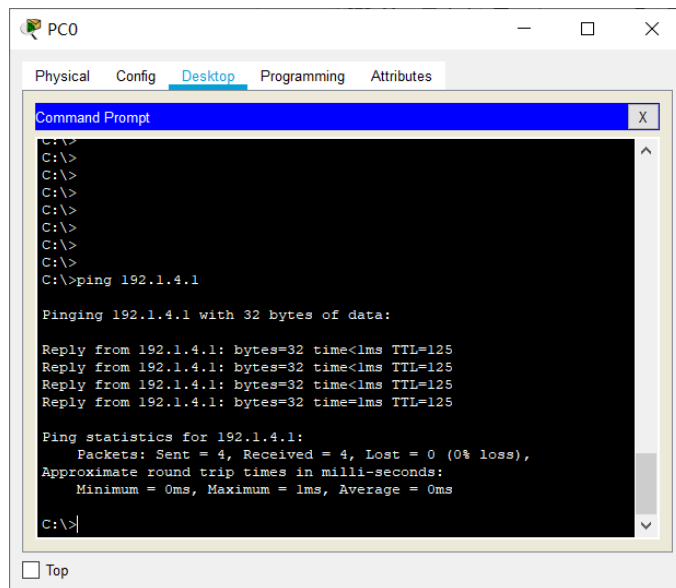
配置后查看路由表（show ip route）



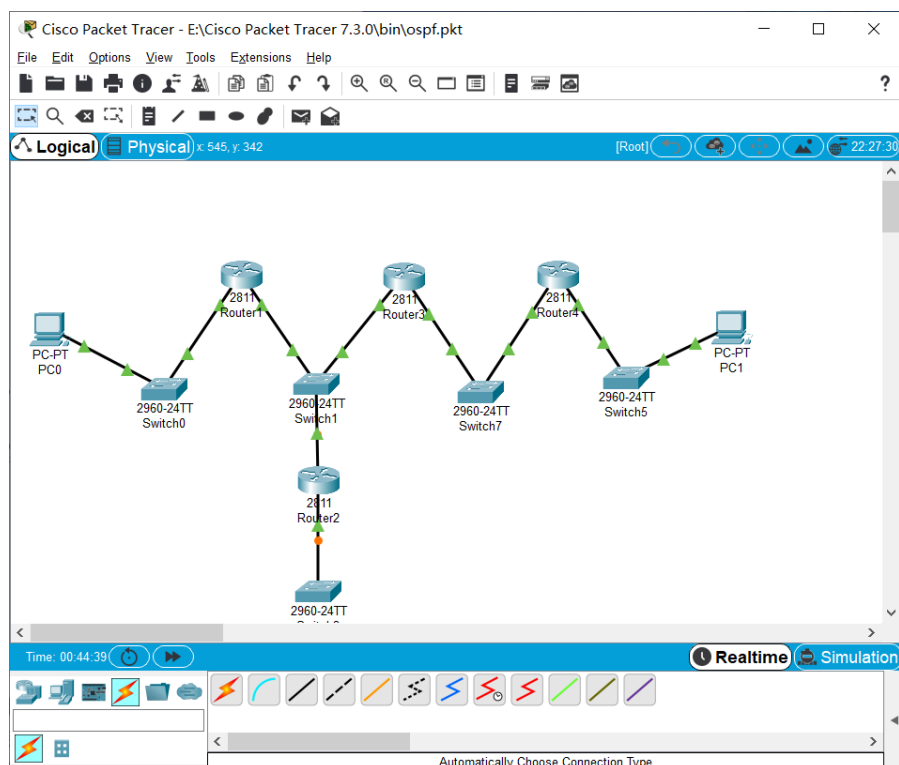
3. 验证 pc0 与 pc1 之间的连通性，如图，已经连通

pc0: 192.1.1.1

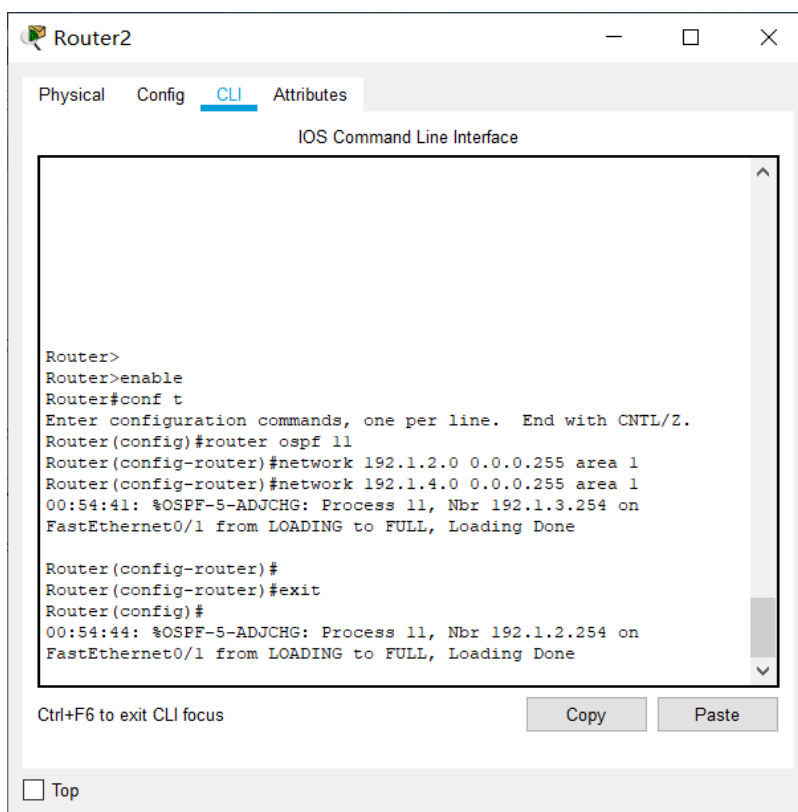
pc1: 192.1.4.1



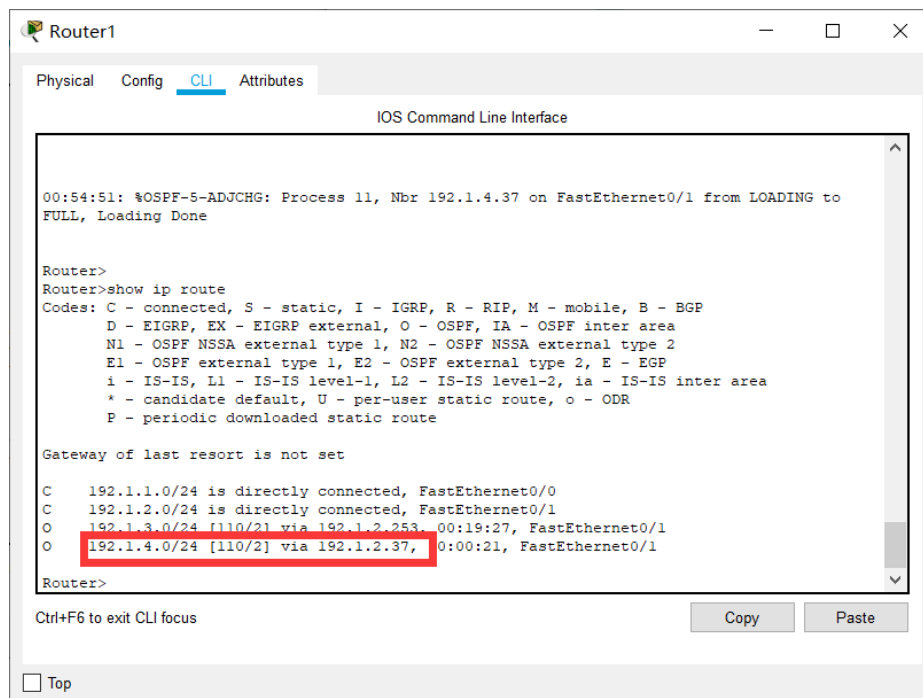
4. 将入侵部分接入网络，如图



给入侵者的路由器 router2 配置 ospf

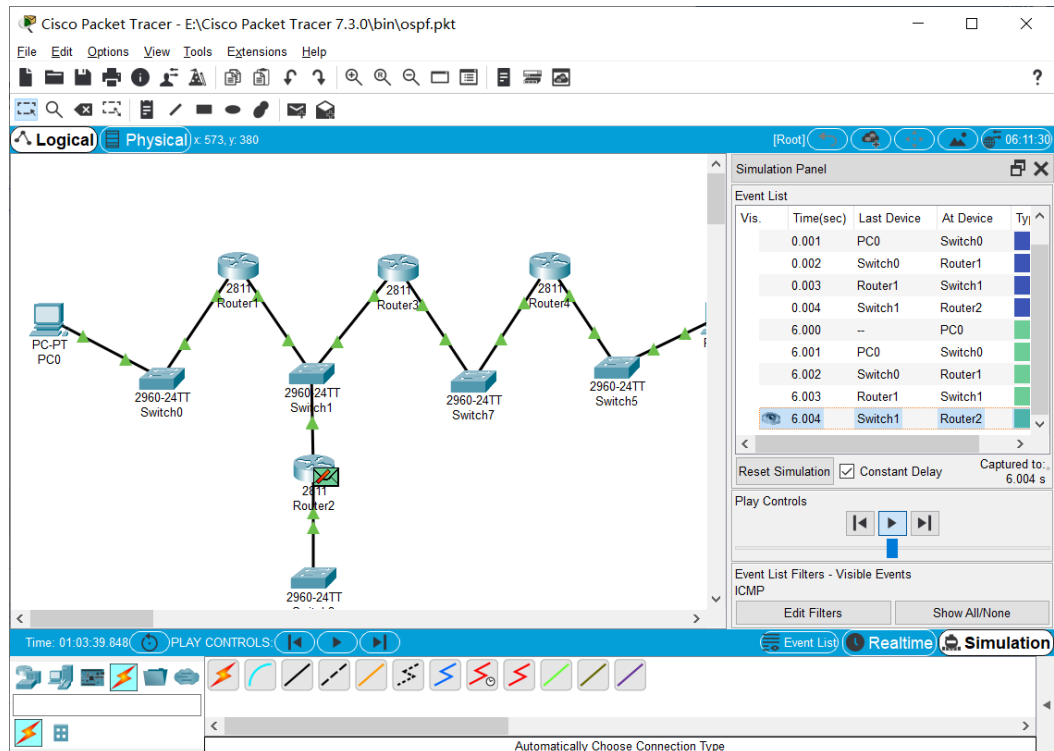


配置完后，查看 router1 的路由表

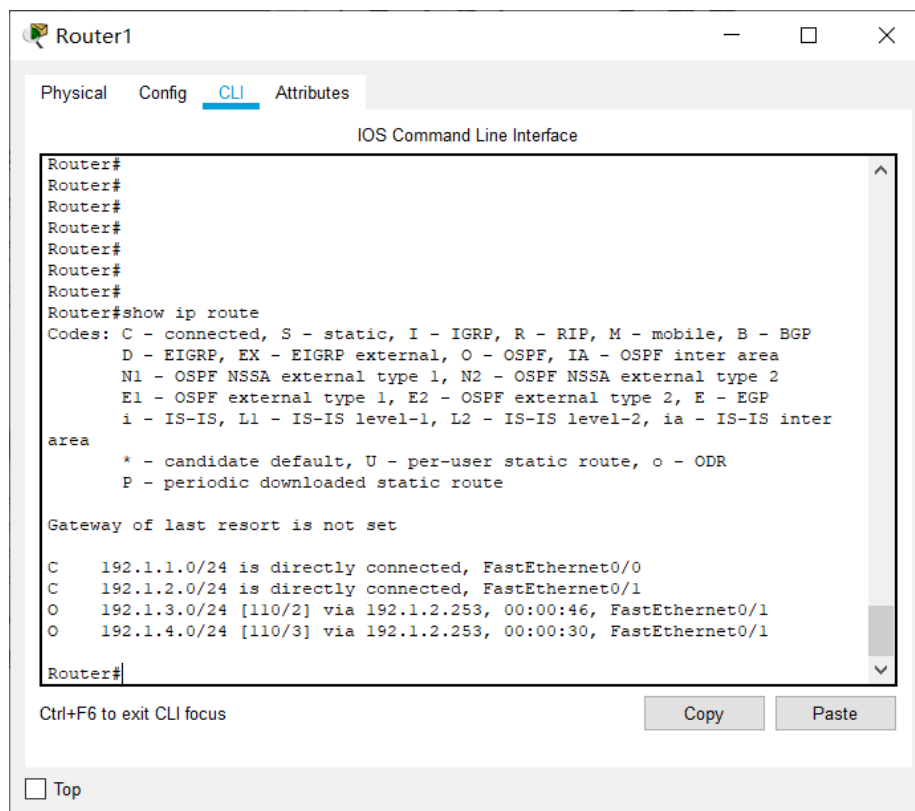


可见前往 192.1.4.0 的下一跳的地址已经变成了入侵者的路由接口地址

5. 进入仿真模式，PC0 发送 ICMP 包给 PC1，可见数据包最终发送给了入侵者的路由，无法到达 PC1



6. 给 router1, router3, router4 添加源端鉴别和完整性检测功能的配置后, 再次查看 router1 的路由表, 可见已经恢复正常



## 五、 实验分析总结及心得

通过这次实验，我对 OSPF 这方面的安全知识有了新的认识，学会了防御这些攻击的基本操作，对它们的攻击流程有了一个清晰的认识。也对这路由表的转发模式这个概念有了更深入的理解，明白了给配置路由消息携带鉴别码的重要性，提高了自己的安全意识。



## 实验二 流量管制实验

### 六、 实验目的

1. 验证流量管制器的配置过程。
2. 验证通过流量管制阻止病毒快速传播的过程。
3. 验证通过流量管制阻止拒绝服务攻击的过程。
4. 验证流量管制的工作原理。

### 七、 实验原理

实施流量管制的前提有两个:一是分类信息流,从图 6.18 中的路由器 R1 接口 2 和路由器 R2 接口 1 输出的信息流中分离出网络 192.1.1.0/24 和网络 192.1.3.0/24 中的终端发送给邮件服务器和 Web 服务器的流量;二是限定这些流量的平均传输速率。

通过规则从 IP 分组流中鉴别出一组 IP 分组,规则由一组属性值组成,如果某个 IP 分组携带的信息和构成规则的一组属性值匹配,意味着该 IP 分组和该规则匹配。构成规则的属性值通常由下述字段组成:

- (1)源 IP 地址,用于匹配 IP 分组 IP 首部中的源 IP 地址字段值。
- (2)目的 IP 地址,用于匹配 IP 分组 IP 首部中的目的 IP 地址字段值。
- (3)源和目的端口号,用于匹配作为 IP 分组净荷的传输层报文首部中源和目的端口号字段值。
- (4)协议类型,用于匹配 IP 分组首部中的协议字段值。

例如分离出网络 192.1.1.0/24 中的终端发送给邮件服务器的流量的规则如下:(1)协议类型=TCP。

- (2)源 IP 地址=192.1.1.0/24。
- (3)源端口号:任意。
- (4)目的 IP 地址=193.1.2.3/32。
- (5)目的端口号=25。

限制流量平均传输速率采用如图 6.19 所示的令牌桶算法。如果授予每一个令牌 P 字节的传输能力,且令牌生成器生成令牌的速率是 R 个令牌/s,则平均传输速率= $P \times 8 \times R$ 。

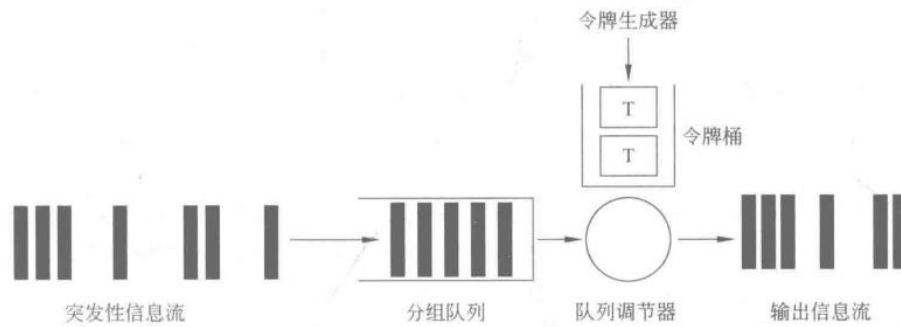
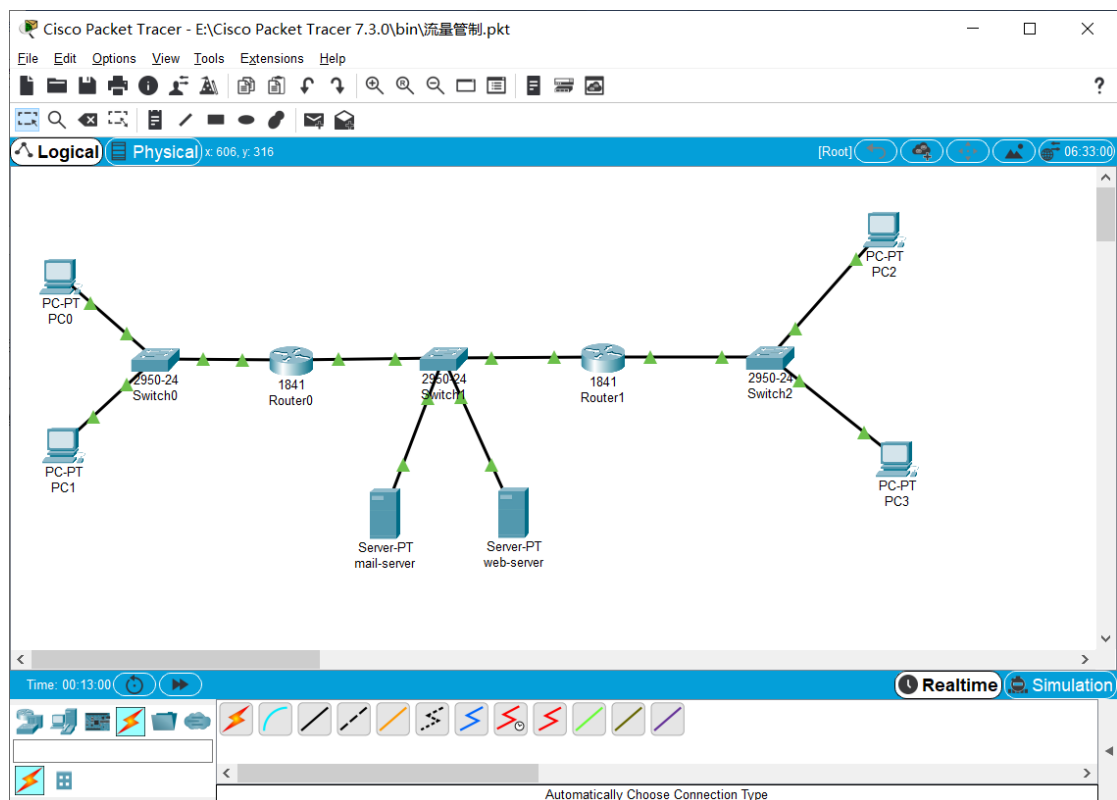


图 6.19 令牌桶算法操作过程

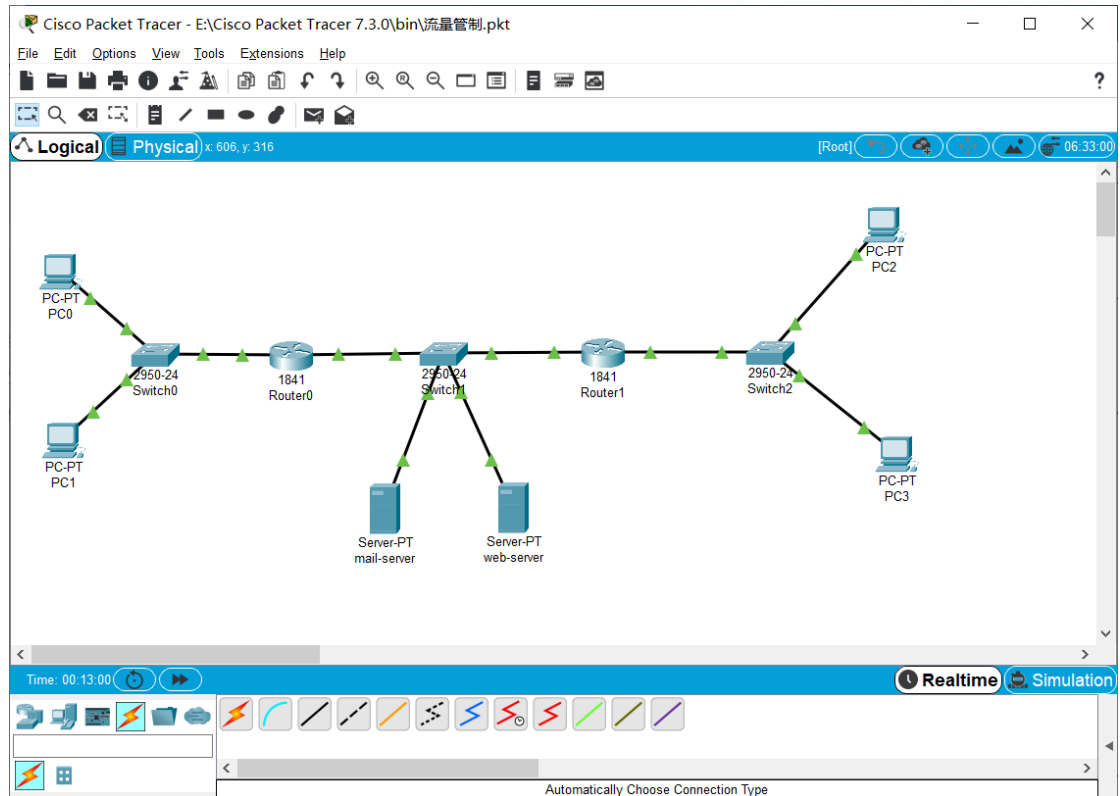
如果授予每一个令牌的传输能力是不变的,可以通过改变令牌生成器生成令牌的速率改变平均速率。  
假定授予每一个令牌  $P$  字节的传输能力,如果设定的平均传输速率是  $V_{iups}$ ,则生成令牌的速率  $= V / (P \times 8)$ 。

## 八、 实验环境/实验拓扑图

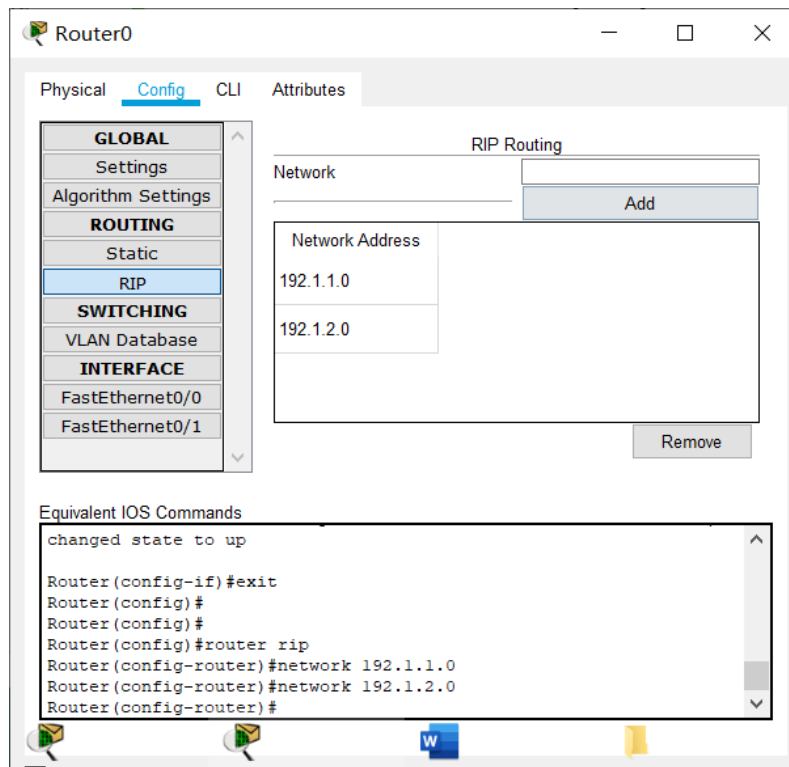


## 九、 主要操作步骤及实验结果记录

1. 完成拓扑图连接



2. 完成接口的 IP、掩码配置。为 router0 和 router1 配置 RIP，其中 router0 配置如下，router 类似



配置完后二者的路由表分别如下

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```

Router>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.1.0/24 is directly connected, FastEthernet0/0
C    192.1.2.0/24 is directly connected, FastEthernet0/1
R    192.1.3.0/24 [120/1] via 192.1.2.253, 00:00:01, FastEthernet0/1

Router>

```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```

%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    192.1.1.0/24 [120/1] via 192.1.2.254, 00:00:12, FastEthernet0/0
C    192.1.2.0/24 is directly connected, FastEthernet0/0
C    192.1.3.0/24 is directly connected, FastEthernet0/1

Router#

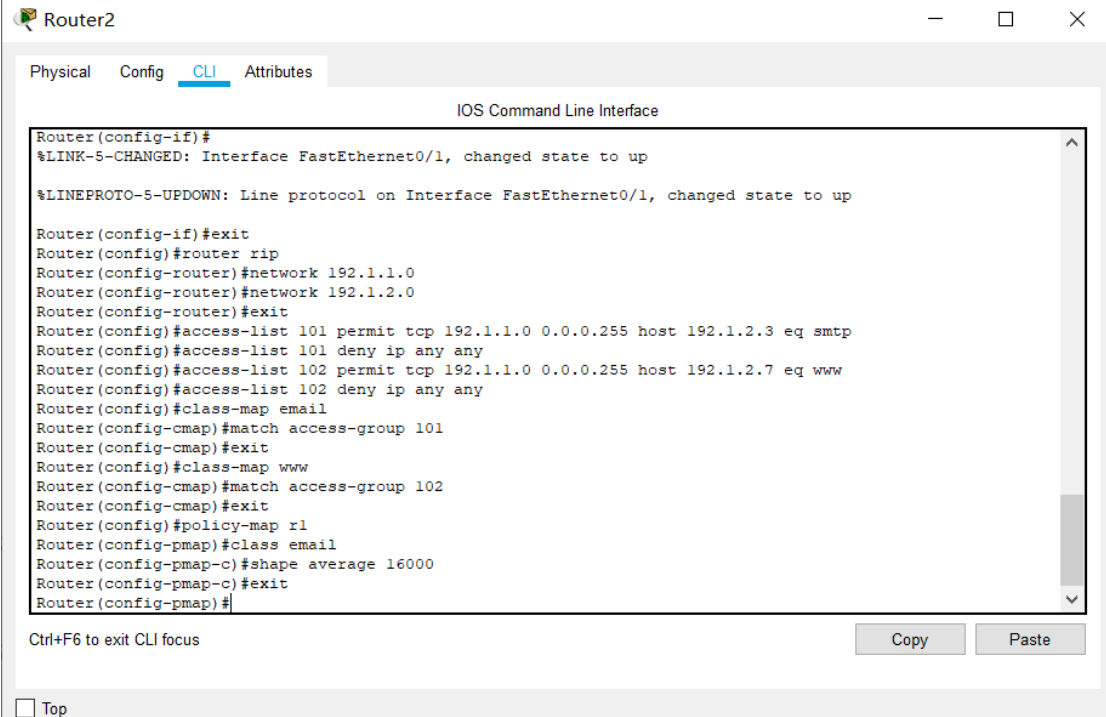
```

Ctrl+F6 to exit CLI focus

Copy Paste

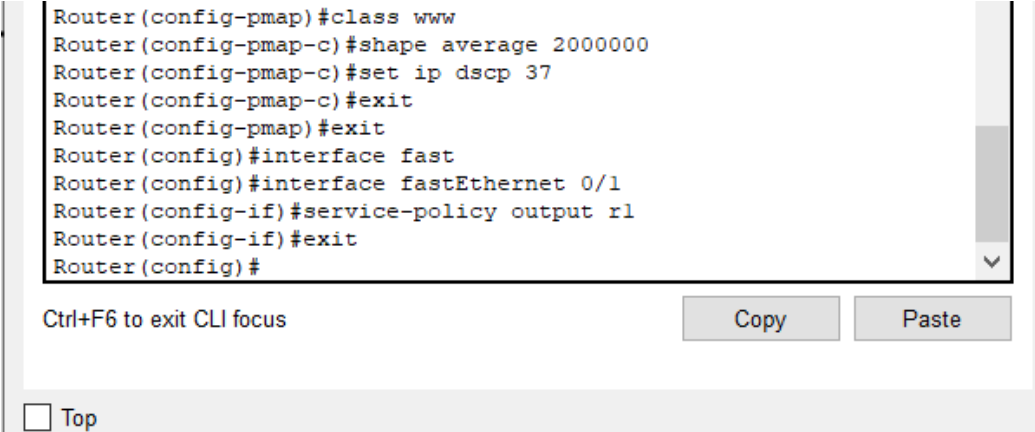
☐ Top

3. 完成各个终端的信息配置
4. 完成路由器 router1, router2 流量管制器的配置, 将 192.1.1.0/24 网段中的终端向 email 服务器发送的平均流量限制为 16000bps。向 web 服务器发送的流量限制为 2000000bps



The screenshot shows the 'Router2' window with the 'CLI' tab selected. The 'IOS Command Line Interface' text is centered above the command input area. The command history shows the configuration of interfaces, IP addresses, access lists, and class maps for traffic shaping. The current command is 'Router(config-pmap-c)#'. Below the command area are 'Copy' and 'Paste' buttons, and a 'Top' button at the bottom left.

```
Router2
Physical Config CLI Attributes
IOS Command Line Interface
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.1.0
Router(config-router)#network 192.1.2.0
Router(config-router)#exit
Router(config)#access-list 101 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq smtp
Router(config)#access-list 101 deny ip any any
Router(config)#access-list 102 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7 eq www
Router(config)#access-list 102 deny ip any any
Router(config)#class-map email
Router(config-cmap)#match access-group 101
Router(config-cmap)#exit
Router(config)#class-map www
Router(config-cmap)#match access-group 102
Router(config-cmap)#exit
Router(config)#policy-map r1
Router(config-pmap)#class email
Router(config-pmap-c)#shape average 16000
Router(config-pmap-c)#exit
Router(config-pmap-c)#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```



This screenshot continues the configuration from the previous one. The command history shows the configuration of the 'www' class map, setting the shape to 2000000, and applying the policy map to the fastEthernet 0/1 interface. The current command is 'Router(config)#'. Below the command area are 'Copy' and 'Paste' buttons, and a 'Top' button at the bottom left.

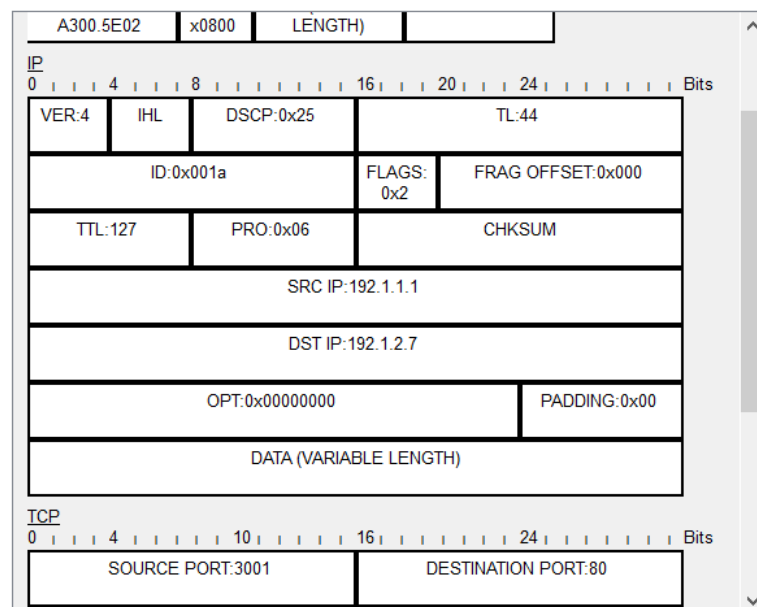
```
Router(config-pmap-c)#class www
Router(config-pmap-c)#shape average 2000000
Router(config-pmap-c)#set ip dscp 37
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#interface fast
Router(config)#interface fastEthernet 0/1
Router(config-if)#service-policy output r1
Router(config-if)#exit
Router(config)#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

进入仿真模拟, pc0 访问 web 服务器的 TCP 报文如下 (操作是打开 pc0 的 web browser 然后一阵狂点 go 按钮)

## PDU Information at Device: Switch1

OSI Model [Inbound PDU Details](#) Outbound PDU Details

### PDU Formats



因流量管制而被丢弃的包

## PDU Information at Device: Router2

OSI Model [Inbound PDU Details](#) Outbound PDU Details

At Device: Router2  
Source: PC0  
Destination: 192.1.2.7

### In Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.1.1.1, Dest. IP: 192.1.2.7
Layer 2: Ethernet II Header 0030.F2E4.363E >> 0030.A300.5E01
Layer 1: Port FastEthernet0/0

### Out Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.1.1.1, Dest. IP: 192.1.2.7
Layer 2: Ethernet II Header 0030.A300.5E02 >> 0001.4329.D9B3
Layer 1: Port(s):

1. Packet exceeded shape limit and dropped.

Challenge Me

<< Previous Layer

Next Layer >>

5. 将前往 web server 的浏览器的流量速率限制为 2000000bps,

```

Router(config)#policy-map rl
Router(config-pmap)#class www
Router(config-pmap-c)#shape average 2000000
Router(config-pmap-c)#set ip dscp 37
Router(config-pmap-c)#exit
Router(config-pmap)#

```

Ctrl+F6 to exit CLI focus

Copy

Paste

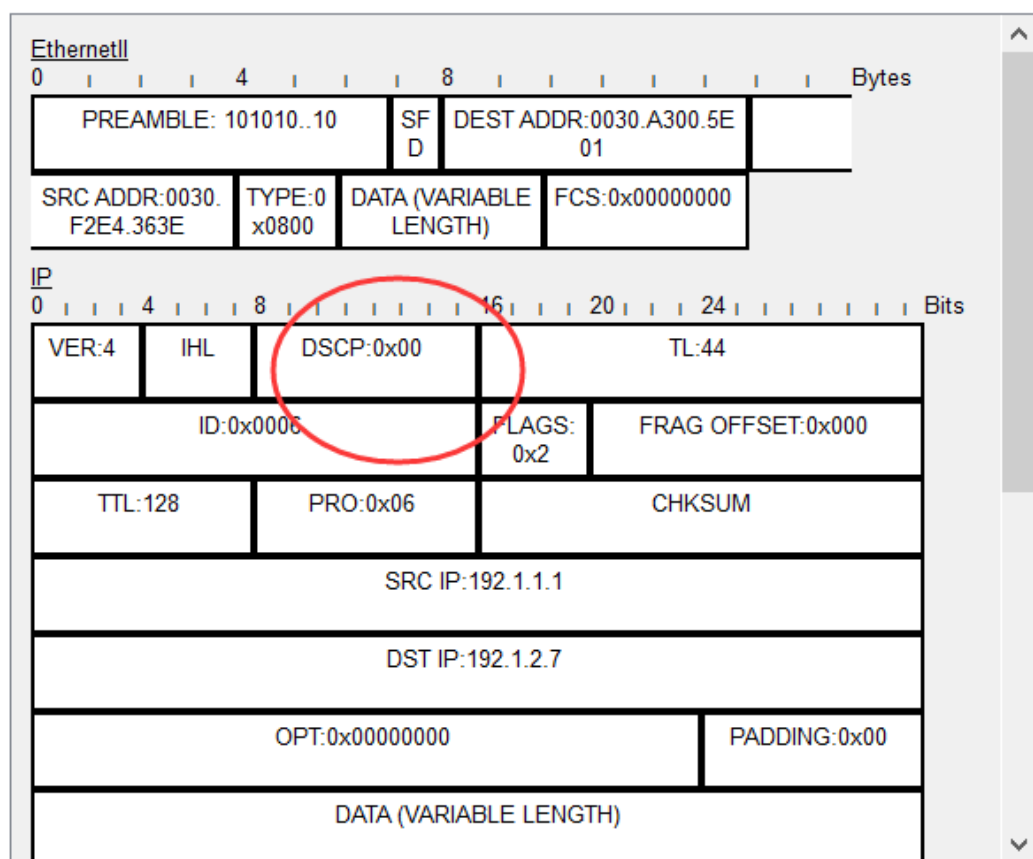
☐ Top

分组前的 ip 首部

## PDU Information at Device: Router2

OSI Model [Inbound PDU Details](#) Outbound PDU Details

### PDU Formats



输出后的 ip 分组首部，0x25 即为之前配置时设置的十进制数值 37

PDU Information at Device: Switch1

OSI Model

Inbound PDU Details

Outbound PDU Details

PDU Formats

EthernetII

0 4 8 Bytes

PREAMBLE: 101010..10

SF D

DEST ADDR:0001.4329.D9 B3

SRC ADDR:0030.A300.5E02

TYPE:0 x0800

DATA (VARIABLE LENGTH)

FCS:0x00000000

IP

0 4 8 16 20 24 Bits

VER:4

IHL

DSCP:0x25

TL:44

ID:0x0006

FLAGS: 0x2

FRAG OFFSET:0x000

TTL:127

PRO:0x06

CHKSUM

SRC IP:192.1.1.1

DST IP:192.1.2.7

OPT:0x00000000

PADDING:0x00

DATA (VARIABLE LENGTH)

## 十、实验分析总结及心得

通过这次实验，我对流量管制这方面的安全知识有了新的认识，学会了防御这些流量攻击的基本操作，对它们的攻击流程有了一个深刻的认识。也对这数据包传输这个概念有了更深入的理解，明白了做好流量管制，提高网站安全防护的重要性提高了自己的安全意识。